

UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

EASTERN DIVISION

CAPITOL RECORDS, INC., a Delaware
corporation; UMG RECORDINGS, INC., a
Delaware corporation; and WARNER BROS.
RECORDS INC., a Delaware corporation,

Plaintiffs,

v.

JOHN DOE,

Defendant.

CIVIL ACTION No.:

04-19490 NG

**DECLARATION OF JONATHAN WHITEHEAD IN SUPPORT OF PLAINTIFFS'
MOTION FOR LEAVE TO TAKE IMMEDIATE DISCOVERY**

I, Jonathan Whitehead, have personal knowledge of the facts stated below and, under penalty of perjury, hereby declare:

1. I am Vice President and Counsel for Online Copyright Protection for the Recording Industry Association of America, Inc. ("RIAA"), where I have been employed for over 6 years. My office is located at 1330 Connecticut Avenue, N.W., Washington, DC 20036. I submit this declaration in support of Plaintiffs' Motion for Leave to Take Immediate Discovery.

2. This declaration is based on my personal knowledge, and if called upon to do so, I would be prepared to testify as to its truth and accuracy.

**The RIAA's Role in Protecting Its Member Recording Industry Companies From
Copyright Infringement**

3. The RIAA is a not-for-profit trade association whose member record companies create, manufacture, and/or distribute approximately ninety percent of all legitimate sound recordings produced and sold in the United States. The RIAA's member record companies comprise the most vibrant national music industry in the world. A critical part of the RIAA's mission is to assist its member companies in protecting their intellectual property in the United States and in fighting against online and other forms of piracy. All of the Plaintiffs in this action are members of the RIAA.

4. The RIAA investigates the unauthorized reproduction and distribution of copyrighted sound recordings online. As Vice President and Counsel for Online Copyright Protection, I am responsible for formulating and implementing online strategies for the RIAA, including investigations into the online infringement of copyrighted sound recordings of all kinds.

The Internet and Music Piracy

5. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows hundreds of millions of people around the world to communicate freely and easily and to exchange ideas and information, including academic research, literary works, financial data, music, movies, graphics, and an unending and ever-changing array of other data. Unfortunately, the Internet also has afforded opportunities for the wide-scale piracy of copyrighted sound recordings and musical compositions. Once a sound recording has been transformed into an unsecured digital format, it can be copied further and

distributed an unlimited number of times over the Internet, without significant degradation in sound quality.

6. Much of the unlawful distribution of copyrighted sound recordings over the Internet occurs via “peer-to-peer” (“P2P”) file copying networks or so-called online media distribution systems. The most notorious example of such a P2P system was Napster, which was enjoined by a federal court. In addition, there are many other P2P networks, including KaZaA, eDonkey, iMesh, Grokster, and Gnutella, that continue to operate and to facilitate widespread copyright piracy. The major recording companies are currently engaged in litigation against KaZaA and Grokster. At any given moment, millions of people illegally use online media distribution systems to upload or download copyrighted material.

7. P2P networks, at least in their most popular form, refer to computer systems or processes that enable Internet users to: (1) make files (including audio recordings) stored on a computer available for copying by other users; (2) search for files stored on other users’ computers; and (3) transfer exact copies of files from one computer to another via the Internet. P2P networks enable users who otherwise would have no connection with, or knowledge of, each other to offer to each other for distribution and copying files off of their PCs, to provide a sophisticated search mechanism by which users can locate these files for downloading, and to provide a means of effecting downloads.

8. The major record companies generally have not authorized their copyrighted sound recordings to be copied or distributed in unsecured formats by means of P2P

networks. Thus, the vast majority of the content that is copied and distributed on P2P networks is unauthorized by the copyright owner — that is, the distribution violates the copyright laws.

9. The scope of online piracy of copyrighted works cannot be underestimated. Retail sales — the principal revenue source for most record companies — declined 7% in 2000, 10% in 2001, and 11% in 2002. The RIAA member companies lose significant revenues on an annual basis due to the millions of unauthorized downloads and uploads of well-known recordings that are made available on the Internet by infringers who, in virtually all cases, have the ability to maintain their anonymity to all but the Internet Service Provider (“ISP”) they use to supply them with access to the Internet.

10. In contrast to the terrible harm to copyright owners, ISPs likely benefit from P2P networks. Those who would unlawfully upload and download copyrighted music often use large amounts of bandwidth (because music files are so large). The infringers thus tend to subscribe to services, such as DSL and cable modems, that are far more expensive than ordinary telephone services. One publication recently estimated that 50-70 percent of the bandwidth of cable broadband network was being used for P2P file copying. See Alan Brezneck, “Service Control Vendors vie for MSO Business,” *Cable Datacom News* (March 1, 2003).

11. The persons who commit infringements by using the P2P networks are, by and large, anonymous to Plaintiffs. A person who logs on to a P2P network is free to use any alias (or computer name) whatsoever, without revealing his or her true identity to other users.

Thus, Plaintiffs can observe the infringement occurring on the Internet, but do not know the true names or mailing addresses of those individuals who are committing the infringement.

The RIAA's Identification of Copyright Infringers

12. In order to assist its members in combating copyright piracy, the RIAA conducts searches of the Internet, as well as file-copying services, for infringing copies of sound recordings whose copyrights are owned by RIAA members. A search can be as simple as logging onto a P2P network and examining what files are being offered by others logged onto the network. These searches generally result in the identification of specific Internet Protocol ("IP") addresses from which infringers are making unauthorized copies of sound recordings available to the public. An IP address is a unique identifier that, along with the date and time, specifically identifies a particular computer or server using the Internet. An IP address also allows the RIAA to use publicly available databases to ascertain, in general terms, the ISP that provides the infringer with access to the Internet.

13. The RIAA engages in a painstaking process to determine whether a person is infringing. That process relies on human review of evidence supporting the allegation of infringement. For each suspected infringer, the RIAA reviews a listing of the music files that the user has offered for upload by others from his or her computer in order to determine whether they appear to be copyrighted sound recordings. The RIAA also downloads copyrighted sound recordings from these users, and listens to them in order to confirm that they are, indeed, illegal copies of sound recordings whose copyrights are owned by RIAA members. The RIAA also downloads and stores other evidence, such as metadata accompanying each file being disseminated that demonstrates that the user is engaged in copyright infringement.

14. The RIAA frequently has used the subpoena processes of Federal Rule of Civil Procedure 45 and the Digital Millennium Copyright Act ("DMCA") to obtain the names of infringers from ISPs. (Individuals only can gain access to the Internet after setting up an account with, or subscribing to, an ISP.) The RIAA typically has included in their subpoenas to ISPs an IP address and a date and time on which the RIAA observed use of the IP address in connection with allegedly infringing activity. In some instances, providing the IP address alone to the ISP has been enough to enable the ISP to identify the infringer. Providing the date and time further assists some ISPs in identifying infringers, especially ISPs that use "dynamic IP addressing" such that a single computer may be assigned different IP addresses at different times, including, for example, each time it logs into the Internet.⁴ Once provided with the IP address, plus the date and time of the infringing activity, the infringer's ISP quickly and easily can identify the computer from which the infringement occurred (and the name and address of the subscriber that controls that computer), sometimes within a matter of minutes.

15. Since 1998, the RIAA and others have used subpoenas thousands of times to learn the names, addresses, telephone numbers, and e-mail addresses of infringers for the purpose of bringing legal actions against those infringers. During a recent litigation with Verizon (an ISP) relating to the DMCA subpoena process, Verizon conceded that, as an alternative to the DMCA process, Plaintiffs could file "John Doe" lawsuits and issue Rule 45 subpoenas to ISPs to obtain the true identities of infringing subscribers.

⁴ ISPs own or are assigned certain blocks or ranges of IP addresses. An ISP assigns a particular IP address in its block or range to a subscriber when that subscriber goes "online."

The RIAA's Identification of the Infringers in This Case

16. In the ordinary course of investigating online copyright infringement, the RIAA became aware that the Defendant was offering files for download on a P2P network. The user-defined author and title of the files offered for download by the Defendant suggested that many were copyrighted sound recordings being disseminated without the authorization of the copyright owners. The RIAA downloaded and listened to a representative sample of the music files being offered for download by the Defendant and was able to confirm that the files he or she was offering for distribution were illegal copies of sound recordings whose copyrights are owned by RIAA members. The RIAA also recorded the time and date at which the infringing activity was observed and the IP address assigned to the Defendant at the time. See Complaint Exhibit A. The RIAA could not, however, determine the physical location of the user or his or her identity. The RIAA could determine that the Defendant was using Northeastern University's service to distribute and make available for distribution the copyrighted files.

17. The RIAA also has collected for the Defendant a list of the files he or she has made available for distribution to the public. Exhibit 1 to this Declaration is this list. This list shows hundreds of files, many of which are sound recording (MP3) files that are owned by, or exclusively licensed to, Plaintiffs.

The Importance of Expedited Discovery in This Case

18. Obtaining the identity of copyright infringers on an expedited basis is critical to stopping the piracy of RIAA members' copyrighted works.

19. First, every day that copyrighted material is disseminated without the authorization of the copyright owner, the copyright owner is economically harmed. Prompt identification of infringers is necessary in order for copyright owners to take quick action to stop unlawful dissemination of their works and minimize their economic losses.

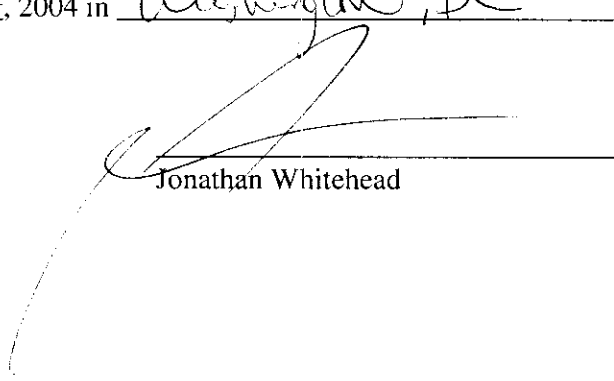
20. Second, infringement often occurs with respect to sound recordings that have not yet been distributed publicly. Such infringement inflicts great harm on the initial market for new works. New recordings generally earn a significant portion of their revenue when they are first released, and copyright piracy during a recording's pre-release or early release period therefore deprives copyright owners of an important opportunity to reap the benefits of their labor.

21. Third, without expedited discovery Plaintiffs have no way of serving Defendant with the complaint and summons in this case. Plaintiffs do not have the Defendant's name or address, nor do they have an e-mail address for Defendant.

22. Fourth, and perhaps most critically, service providers have different policies pertaining to the length of time they preserve "logs" which identify their users. ISPs keep log files of their user activities for only limited periods of time – which can range from as short as a few days, to a few months – before erasing the data they contain. If an ISP does not respond expeditiously to a discovery request, the identification information in the ISP's logs may be erased, making it impossible for the ISP to determine the identity of the infringer and eliminating the copyright owner's ability to take action to stop the infringement.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed on November 12, 2004 in Washington, DC.



Jonathan Whitehead

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

CLERK'S NOTICE

This document can not be scanned due to its size, or the way in which it was bound.

The original is available for viewing in the Clerk's Office.